

Møtedato: 20.05.2019
Arkivnr: 2019/1666

Saksbeh/tlf:
Petter B. Hågensen/413 10851

Sted, dato
Mo i Rana, 13.05.2019

Styresak 48– 2019 Informasjonssikkerhet. Status risiko- og sårbarhetsanalyse

Styret i Helgelandssykehuset HF inviteres til å fatte følgende vedtak:

Styret i Helgelandssykehuset HF tar saken til orientering

Formål:

Orienterer styret om status på risiko- og sårbarhetsanalyser om informasjonssikkerhet

Bakgrunn/Sammendrag:

I Oppdragsdokumentet 2019, punkt 4.2.2 Personvern og informasjonssikkerhet, er det krav til å styrebehandle status på risiko- og sårbarhetsanalyser om informasjonssikkerhet innen 1. juni.

Helgelandssykehuset har etter rapporter fra riksrevisjonen gjennomført risikovurderinger i eget foretak og i samarbeid med de andre foretakene i Helse Nord. Det har blant annet blitt avdekket manglende gjennomføring av kontroll av innsynslogg.

Helgelandssykehuset har siden medio 2018 hatt fokus på å registrere inn, og skaffe oversikt over de behandlingene av helse og personopplysninger som finner sted i Helgelandssykehuset. Dette har vært og er et møysommelig arbeid som både personvernombud og informasjonssikkerhetsrådgiver har jobbet med og registrert inn i systemet: Personvernapp. I denne oversikten skal ROS-analyser og Personvernkonsekvensvurdering (DPIA'er) også legges inn.

I de gjennomførte ROS-analysene ser vi følgende risikoer:

1. Systematisk kontroll av innsyn i journaler. Helgelandssykehuset har ikke fått gjennomført tilstrekkelig mange nok egenkontroller av innsyn i journaler. Krav i våre prosedyrer er at dette skal gjennomføres 4 ganger pr. år. Tiltak som vurderes er å overføre deler av denne kontrollen til kontortjenesten. Det pågår også et arbeid med å innføre felles nasjonal løsning for å automatisere denne kontrollen. Ferdigdato er ikke satt.
2. Kontroll av ansattes tilganger. Det er mangler i kontrollen av ansattes tilganger, spesielt ved flytting av arbeidsområde. Kontrollen gjennomføres ikke systematisk. Ansvar ligger i hovedsak på nærmeste leder. I det pågående HIS-prosjektet (Helhetlig informasjonssikkerhet) vil det bli etablert, kanskje allerede i år et nytt system som skal ivareta denne utfordringen på en bedre måte.

3. Bevisstgjøring ved bruk av e-post. E-post fra avsendere som utgir seg for å være noen andre enn de faktisk er, kan inneholde enten vedlegg eller linker til sider som kan føre til at mottaker blir utsatt for ondartete handlinger. De hendelsene som til nå er rapportert inn har blitt avverget, men vi ser en økning i antall ondartete e-poster. Her er tiltak e-læringskurs, informasjonsmøter ute på avdelingene, samt brukertips som jevnlig skal komme på intranettsiden for informasjonssikkerhet.

Videre plan for gjennomføring av ROS-analyser vil i hovedsak dreie seg om konkrete behandlinger/forløp i DIPS Classic og DIPS Arena til høsten, dette er de systemene som omfatter flest brukere og som berører flest pasienter.

Mo i Rana, 13. mai 2019

Hulda Gunnlaugsdottir
Administrerende direktør